Some design theoretic results on the Conway group ·0

Ben Fairbairn

School of Mathematics
University of Birmingham, Birmingham, B15 2TT, United Kingdom

fairbaib@maths.bham.ac.uk

Submitted: Oct 3, 2008; Accepted: Jan 14, 2010; Published: Jan 22, 2010
Mathematics Subject Classification: 05B99, 05E10, 05E15, 05E18

Abstract

Let Ω be a set of 24 points with the structure of the (5,8,24) Steiner system, $\mathcal{S}$, defined on it. The automorphism group of $\mathcal{S}$ acts on the famous Leech lattice, as does the binary Golay code defined by $\mathcal{S}$. Let $A, B \subset \Omega$ be subsets of size four ("tetrads"). The structure of $\mathcal{S}$ forces each tetrad to define a certain partition of Ω into six tetrads called a sextet. For each tetrad Conway defined a certain automorphism of the Leech lattice that extends the group generated by the above to the full automorphism group of the lattice. For the tetrad A he denoted this automorphism ζ_A. It is well known that for ζ_A and ζ_B to commute it is sufficient to have A and B belong to the same sextet. We extend this to a much less obvious necessary and sufficient condition, namely ζ_A and ζ_B will commute if and only if $A \cup B$ is contained in a block of $\mathcal{S}$. We go on to extend this result to similar conditions for other elements of the group and show how neatly these results restrict to certain important subgroups.

1 Introduction

The Leech lattice, Λ, was discovered by Leech in 1965 in connection with the packing of spheres into 24-dimensional space $\mathbb{R}^{24}$, so that their centres form a lattice. Its construction relies heavily on the rich combinatorial structure of the Mathieu group M_{24}. Leech himself considered the group of symmetries fixing the origin 0; he had enough geometric evidence to predict the order of this group to within a factor of two, but could not prove the existence of all the symmetries he anticipated. John Conway subsequently produced a beautifully simple additional symmetry of Λ and in doing so determined the order of the group it generated together with the monomial subgroup used in the construction of Λ (see [3]). He proved that this is the full group of symmetries of Λ fixing the origin; that it was perfect; had centre of order two and that the quotient by its centre was simple.

In this paper we give a combinatorial condition that enables one to immediately see with minimal effort when Conway's additional symmetries of ·0 commute. As we shall

see this is readily adapted to analogous conditions for other elements of the group and to certain subgroups.

In Section 2 we recall some notation along with the basic construction of the Leech lattice and the group $\cdot 0$. In Section 3 we state and prove our main theorem. In Section 4 we use this to prove a similar result for the 'Golay codewords', as defined in Section 2. In Section 4 we show how these results may be readily adapted for use with other elements. Finally in Section 5 we see how these results restrict to some subgroups of $\cdot 0$.

2 The Leech Lattice and $\cdot 0$

In this section we shall define the Leech lattice and the Conway group $\cdot 0$. We will closely follow the account given by Conway [4] which may be found in Conway and Sloane [6, Chapter 10].

A Steiner system, $\mathcal{S}(5,8,24)$, is a collection of 759 8-element subsets of a 24-element set, Ω, known as *octads*, with the property that any 5-element subset of Ω is contained in precisely one octad. It turns out that such a system is unique up to relabeling and the group of permutations of Ω that preserve such a system is a copy of the sporadic simple Mathieu group M_{24} which acts 5-transitively on the 24 points of Ω. Moreover the set of all octads passing through a fixed point of Ω will form a Steiner system $\mathcal{S}(4,7,23)$ defined analogously to $\mathcal{S}(5,8,24)$ whose automorphism group is the sporadic group M_{23}. Similarly a fixed pair of points define a Steiner system $\mathcal{S}(3,6,22)$ and the sporadic group M_{22}.

The symmetric difference of two octads that intersect in four points may be shown to be another octad. Consequently the 24 points of Ω can be partitioned into 6 complementary *tetrads* (4-element subsets) such that the union of any two of them is an octad. Such a partition is called a *sextet*.

Let $\mathbb{P}(\Omega)$ denote the powerset of Ω regarded as a 24-dimensional vector space over the field of two elements, $\mathbb{F}_2$. The subspace spanned by the 759 octads contains the empty set; the 759 octads; 2576 12-element subsets known as *dodecads*; the 759 complements of the octads, known as 16-*ads*, and the whole set Ω. This is a 12 dimensional subspace known as the *Binary Golay code*. We shall denote this $\mathcal{C}_{24}$. We shall further write $\mathcal{C}(8)$ for the octads of $\mathcal{C}_{24}$ and $\mathcal{C}(12)$ for the dodecads. We define the *weight* of a codeword to be its number of non-zero components.

A much used approach to this Steiner system is the Miracle Octad Generator (MOG) discovered by Curtis [7]. A more modern account is given in [6, Chapter 11]. Since we shall make great use of this important piece of notation we shall describe it here in some detail.

The MOG is an arrangement of the 24 points of Ω into a 4×6 array in which the octads assume a particularly recognizable form; so it is easy to read them off. Naturally the six columns of the MOG, that we label $1,\ldots,6$, will form a sextet. The pairing of the columns $12\cdot 34\cdot 56$ are known as the *bricks* of the MOG. The *Hexacode*, $\mathcal{H}$, is a 3-dimensional quarternary code of length six whose codewords give an algebraic notation for the binary codewords of $\mathcal{H}$ as given in the MOG. Explicitly if $\{0,1,\omega,\bar{\omega}\}=K\cong\mathbb{F}_4$, then

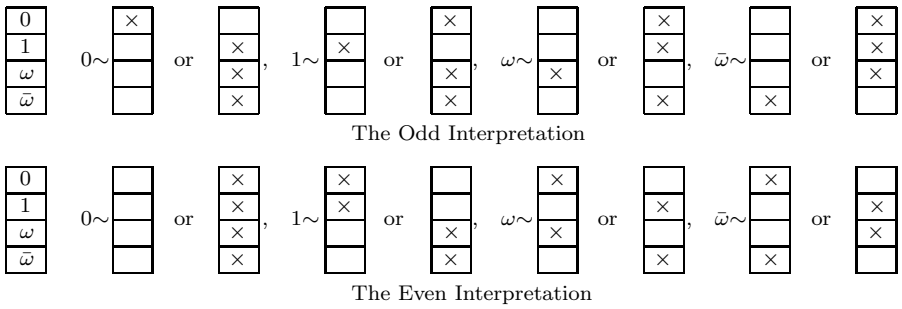


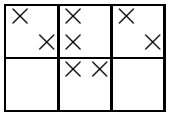
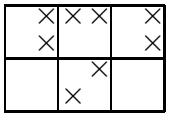
Figure 1: The odd and even interpretations of hexacode words

$$\begin{aligned}\mathcal{H} &= \langle (1,1,1,1,0,0),(0,0,1,1,1,1),(\bar{\omega},\omega,\bar{\omega},\omega,\bar{\omega},\omega)\rangle \\ &= \{(0,0,0,0,0,0)\text{ (1 such)},(0,0,1,1,1,1)\text{ (9 such)},\\ &\quad (\bar{\omega},\omega,\bar{\omega},\omega,\bar{\omega},\omega)\text{ (12 such)},\\ &\quad (\bar{\omega},\omega,0,1,0,1)\text{ (36 such)},(1,1,\omega,\omega,\bar{\omega},\bar{\omega})\text{ (6 such)}\}\end{aligned}$$

where multiplication by powers of ω are of course allowed, as is an S_4 of permutations of the coordinates corresponding to the symmetric group $S_4 \cong \langle (135)(246),(12)(34),(13)(24)\rangle$ (the even permutations of the wreath product of shape $2 \wr S_3$ fixing the pairing $12 \cdot 34 \cdot 56$). Each hexacode word has an *even* and *odd* interpretation and each interpretation corresponds to 2^5 binary codewords in $\mathcal{H}$, giving the $2^6 \times 2 \times 2^5 = 2^{12}$ binary codewords of $\mathcal{C}_{24}$. The rows of the MOG are labeled in descending order with the elements of K as shown in Figure 1, thus the top row is labeled 0.

Let $(h_1,\ldots,h_6) \in \mathcal{H}$. Then in the odd interpretation, if $h_i = \lambda \in K$ we place a 1 in the λ position in the i^{th} column and zeros in the other three positions, or we may complement this and place 0 in the λ^{th} position and 1s in the other three positions. We do this for each of the 6 values of i and may complement freely so long as the *the number of 1s in the top row is odd*. So there are 2^5 choices.

In the even interpretation if $h_i = \lambda \neq 0$ we place 1 in the 0^{th} and λ^{th} positions and zeros in the other two, so as before we may complement. If $h_i = 0$ then we place 0 in all four positions or 1 in all four positions. This time we may complement freely so long as *the number of 1s in the top row is even*. Thus for instance

$(0,1,\bar{\omega},\omega,0,1) \sim$  or 

24	23	11	1	22	2
3	19	4	20	18	10
6	15	16	14	8	17
9	5	13	21	12	7

in the odd and even interpretations respectively, where evenly many complementations are allowed in each case. The last Figure shows the standard labeling of the 24 points of Ω used when entering information into a computer. (One often finds the '23' and '24' replaced with the symbols '0' and '∞' so that the 24 points are labeled using the projective line $P_1(23)$ such that all the permutations of $L_2(23)$ are in M_{24}.) Here we have described the Curtis form of the MOG. To obtain the Conway form of the MOG, also commonly found in the literature, one need only swap over the rightmost two columns.

Following [6], we let $\{e_1, \ldots e_{24}\}$ be an orthonormal basis for $\mathbb{R}^{24}$. Given a set $S \subseteq \Omega$ we write e_S to denote the vectors $\Sigma_{i \in S} e_i$. We shall write Λ_0 for the lattice spanned by the vectors of the form $2e_C$ for $C \in \mathcal{C}(8)$. In Theorem 24 of [4] Conway proves:

Theorem 1 *Λ_0 contains all vectors of the form $4e_T$ ($T \subseteq \Omega$ with $|T| = 4$) and $4e_i \pm 4e_j$ $(i, j \in \Omega, i \neq j)$.*

In particular Λ_0 contains all the vectors of the form $8e_i = (4e_i + 4e_j) + (4e_i - 4e_j), j \neq i$. These vectors are useful for minimizing the amount of work involved in verifying results such as those given here.

The *Leech lattice* is defined to be the lattice spanned by Λ_0 and a vector $u = e_\Omega - 4e_\infty = (-3, 1^{23})$. (Note that $u \notin \Lambda_0$ since the components of all the vectors of Λ_0 are even.) This is well defined since:

	-3	1	1	1	...
+	4	-4	0	0	...
	1	-3	1	1	...

We define the group $\cdot 0$ to be the group of all Euclidean congruences of $\mathbb{R}^{24}$ that fix the origin and preserve the Leech lattice as a whole. We define a *signchange on a set $S \subseteq \Omega$*, ϵ_S, to be a an element of the form:

$$\epsilon_S(e_i) = \begin{cases} -e_i & \text{for } i \in S; \\ e_i & \text{for } i \notin S. \end{cases}$$

Conway found that every element of $\cdot 0$ may be expressed as $\pi \epsilon_C w$ where $\pi \in \mathrm{M}_{24}$, $C \in \mathcal{C}_{24}$ and w is a word of elements that we define as follows. If $A \subset \Omega$ is a tetrad, then let α_A be the operation taking e_i to $e_i - \frac{1}{2} e_B$ where $i \in B \subset \Omega$ and B is in the same sextet as A. In [3] Conway showed that the element $\zeta_A := \alpha_A \epsilon_A$ (defined by extending linearly the action on the basis vectors given for α_A and ϵ_A) is then an automorphism of the Leech lattice not equal to a product of permutations and signchanges. Note that if A and B are distinct tetrads of a given sextet then $\alpha_A = \alpha_B$ but $\zeta_A \neq \zeta_B$. We note that these elements have the following property:

Lemma 2 *If A and B are two distinct tetrads belonging to the same sextet then $\zeta_A \zeta_B = \epsilon_{A \cup B}$*

Proof: $\zeta_A \zeta_B = \alpha_A \epsilon_A \alpha_B \epsilon_B = \alpha_A \alpha_B \epsilon_A \epsilon_B = \epsilon_{A \cup B}$. □

For further details see [6].

3 The Main Theorem

In this section $A, B \subseteq \Omega$ will be tetrads.

Theorem 3 *$\zeta_A \zeta_B = \zeta_B \zeta_A$ if and only if $A \cup B$ is contained in an octad of the Steiner system $\mathcal{S}(5,8,24)$.*

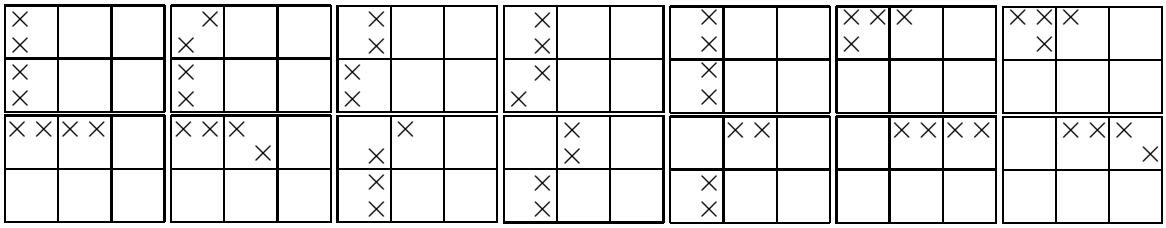


Figure 2: Representatives for the fourteen orbits of B under the action of the stabilizer of A in the group M_{24}

Proof Let $\pi \in \mathrm{M}_{24}$. Clearly the result holds for A and B if and only if it holds for A^π and B^π. It is therefore sufficient to check the result for one member of each orbit of ordered pairs of tetrads (A, B) under the action of M_{24}. Since the action of M_{24} on 24 points is five transitive we may fix A to be the leftmost column of the MOG. By inspecting the possibilities for B we see there are now fourteen orbits to be checked. It remains to verify the result for each of the orbits. We give a representative for each of these orbits in Figure 2.

Now, clearly the result is true if $A = B$. If $A \cup B \in \mathcal{S}(5,8,24)$ then the result is immediate from Lemma 2 since $A \cup B = B \cup A$.

Clearly, a necessary condition for the elements ζ_A and ζ_B to commute is that each of the tetrads A and B intersect each others' sextet in the same manner. Compared to the leftmost column of the MOG, this condition is not met in each of the four cases given in Figure 4. It is thus immediate that none of these will commute with ζ_A for A the leftmost column of the MOG, without any calculation at all. The theorem is therefore true in these cases.

We next observe that if $A \cup B \subset O \in \mathcal{S}(5,8,24)$ then the result will hold whenever $|A \cup B|$=5 if and only if it holds whenever $|A \cup B|$=7 since:

$$\zeta_A\zeta_B = \zeta_A\zeta_B\zeta_{O\setminus B}^2 = \zeta_A\epsilon_O\zeta_{O\setminus B} = \epsilon_O\zeta_{O\setminus B}\zeta_A = \zeta_B\zeta_{O\setminus B}^2\zeta_A = \zeta_B\zeta_A$$

the second and fourth equalities holding by Lemma 2.

The remaining seven cases may all be verified by easy calculation on the vectors of the Leech lattice. As an example of the sort of calculation that's required we give all calculation necessary to verify the result in the unique case with $|A \cup B| = 5$ in Figure 3. □

We remark that theorem 3 has been verified computationally using the programme of [8]. We further remark that the direct calculations performed to verify theorem 3 reveal slightly more is true. Consider the natural 24 dimensional representation of $\cdot 0$. Let χ be the character of this representation. (The full character table of $\cdot 0$ may found in [5, p.184-187].) The character values of each of the 14 possible words $\zeta_A\zeta_B$ depends only on the order of $\zeta_A\zeta_B$. We give these in the Table 5. From this table we can see that many of the words are conjugate to each other. Moreover, they are all conjugate, not only to other words of length two, but to non-fixed point free permutations in M_{24}!

Finally note that since the Leach lattice is defined over $\mathbb{Z}$ it may be used to define modular representations of $\cdot 0$ by reading all vectors mod p. Since this does not effect the

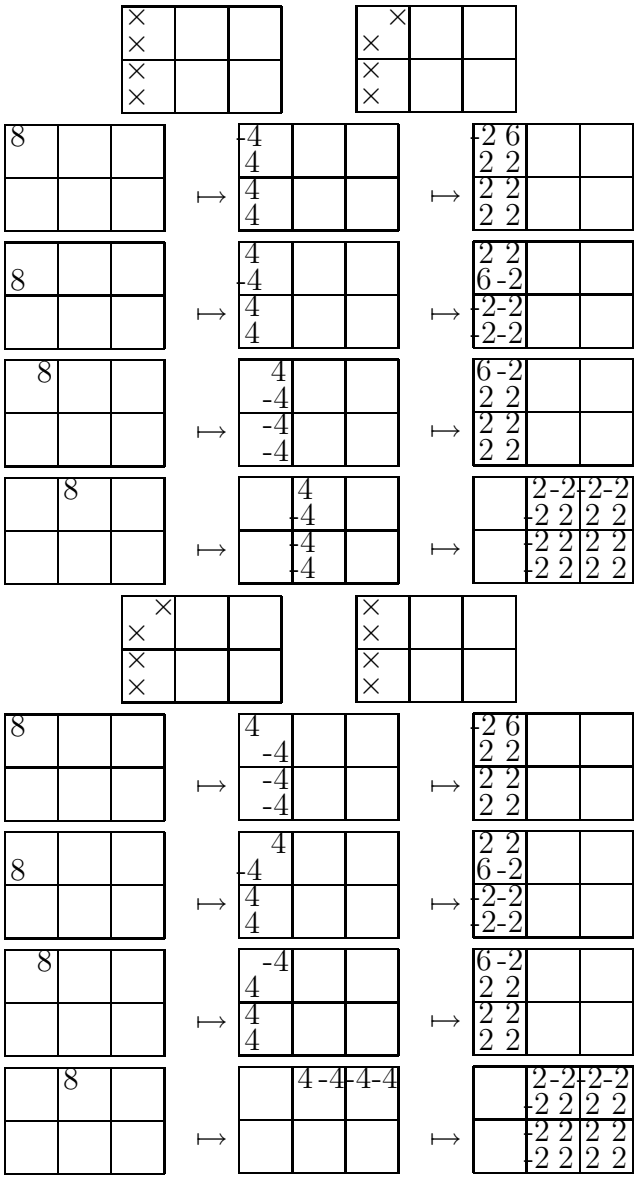


Figure 3: The action of a elements of the form $\zeta_A\zeta_B$ and $\zeta_B\zeta_A$ with $|A \cup B| = 5$ on some vectors of the form $(8,0^{23})$. All other cases are immediate from the above by the high transitivity of M_{24}.

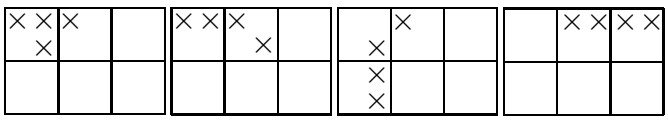


Figure 4: Tetrads whose sextets meet the columns of the MOG, the standard sextet, asymmetrically

$\lvert t_A t_B \rvert$	$\chi(t_A t_B)$
1	24
2	8
3	6
4	4
5	4
6	2

Figure 5: The character values of words of length two

structure of the $\mathcal{S}(5, 8, 24)$ Steiner system or the status of a tetrad as a subset of Ω of size four, the result clearly also hold in any characteristic. Few results of representation theory are completely characteristic free.

4 The Golay codewords

In this section we classify the signchanges on Golay codewords that commute with ζ_T for a given tetrad T. Let $C \in \mathcal{C}_{24}$ be a codeword.

Definition 4 *T is said to* refine *C if either C may be expressed as a union of tetrads of the sextet of T or C is the empty codeword and let T be a tetrad with corresponding element ζ_T.*

Theorem 5 *We have $\zeta_T \epsilon_C = \epsilon_C \zeta_T$ if and only if T refines C.*

Proof First observe that without loss of generality $T \cap C \neq \emptyset$, otherwise if U is a tetrad from the sextet of T meeting C then

$$\zeta_T \epsilon_C = \epsilon_C \zeta_T \Leftrightarrow \epsilon_{U \cup T} \zeta_T \epsilon_C = \epsilon_{U \cup T} \epsilon_C \zeta_T = \epsilon_C \epsilon_{U \cup T} \zeta_T \Leftrightarrow \zeta_U \epsilon_C = \epsilon_C \zeta_U \ (\dagger)$$

since $\epsilon_{U \cup T} = \zeta_U \zeta_T$ by Lemma 2. Next we note that the weight of any binary Golay code word is either 0, 8, 12, 16 or 24. Clearly the theorem holds when C is the empty word (the weight 0 codeword) or ϵ_C is the central involution of $\cdot 0$ (the weight 24 codeword). Now we observe that the result holds for 16-ads if and only if it holds for octads, since one is equal to the other multiplied by the central involution. It remains to prove the result for octads and dodecads.

Again M_{24} act transitively on octads. Moreover the stabiliser of an octad has structure $2^8 : \mathrm{A}_8$, the 2^4 acting regularly on the complementary 16ad and the A_8 acting in a natural way on the 8 points of the octad. Fix a tetrad T and an octad O. By observation (†), we may assume that T meets O and does so in either two, three or four points. If T meets O in four points, then Lemma 2 immediately gives our result since $A \cup B = B \cup A$ for any tetrads A and B. The action of the octad stabilizer in M_{24} is transitive on each of these

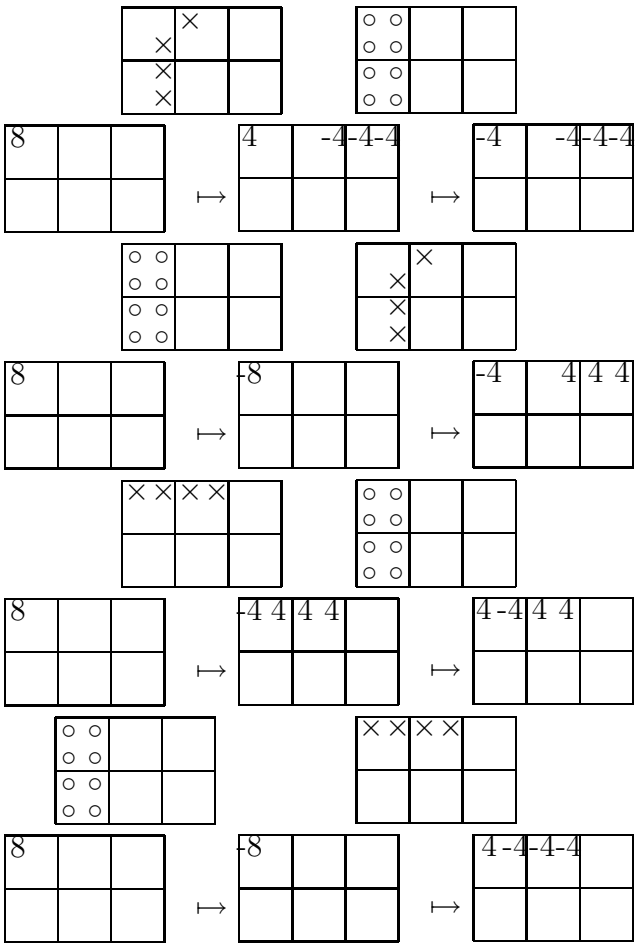


Figure 6: $(\zeta_T \epsilon_O)^2 \neq 1$. Here we use $\times$ to denote the points in a tetrad, T, used to define an element ζ_T and we use $\circ$ to denote the points of an octad, O, used to define a signchange ϵ_O

orbits, so it is sufficient to prove the result for particular choices of T and O. We do this by direct calculation in Figure 6.

Finally it remains to prove the result for dodecads. There are three different possible intersections for a sextet and a dodecad, namely $(1^3, 3^3)$,$(0, 2^4, 4)$ and (2^6). As in the octad case, M_{24} is transitive on dodecads and the stabiliser of a dodecad in this action, which has the structure of the sporadic group M_{12}, is transitive on each of these orbits, so it is sufficient to prove the result in a special case of each of these orbits. We do this in Figure 7. □

5 Other Groups

The results presented here neatly restrict to some of the more interesting subgroups of $\cdot 0$.

Elements of the form $\zeta_T \epsilon_\Omega$ will fix a vector of the form $v := (-3, 1^{23})$ whenever the -3 component of v lies in T. If the -3 component of v is at $i \in \Omega$, then we define a *triad* to be

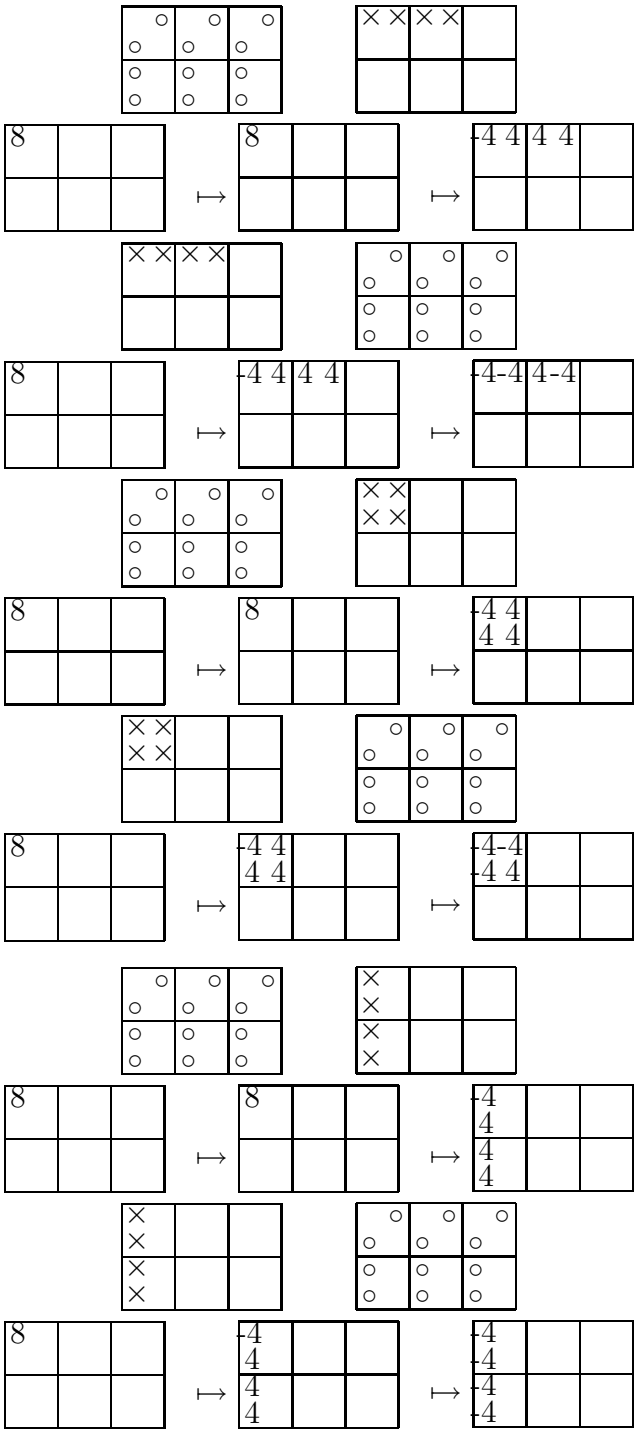


Figure 7: The action of elements of the form $\zeta_T \epsilon_D$ for D a dodecad. Here we again use $\times$ to denote the points in a tetrad, T, used to define an element ζ_T and we use $\circ$ to denote the points of an octad, O, used to define a signchange ϵ_O

any set of size three $R \subseteq \Omega \setminus \{i\}$ and define a *triad element* to be any element of the form $\eta_R := \zeta_{R\cup\{i\}}\epsilon_\Omega$. Any permutation in the stabiliser of i under the action of M_{24}, which has structure M_{23}, will also fix v. Clealy no Golay codewords fix v. Since the central element of $\cdot 0$ is ϵ_Ω we thus have

$$\eta_A\eta_B = \zeta_{A\cup\{i\}}\epsilon_\Omega\zeta_{B\cup\{i\}}\epsilon_\Omega = \zeta_{A\cup\{i\}}\zeta_{B\cup\{i\}}\epsilon_\Omega^2 = \zeta_{A\cup\{i\}}\zeta_{B\cup\{i\}}$$

for any triads A, $B \in \Omega\setminus\{i\}$. Consequently we have as an immediate Corollary of theorem 3:

Corollary 6 *$\eta_A\eta_B = \eta_B\eta_A$ if and only if $A \cup B \subseteq H \in \mathcal{S}(4,7,23)$.*

We thus have a result of the form of theorem 3 in the sporadic group Co_2.

We further find a form of this result in the group $U_6(2)$. Fix $i, j \in \Omega$. The Leech lattice vectors $v_1 := (-3, 1, 1^{22})$, $v_2 := (-1, 3, -1^{22})$, $v_3 := (4, -4, 0^{22})$ are all 2-vectors and have the property that $v_1 + v_2 + v_3 = 0$, the first two components corresponding to the positions i and j. The stabiliser in $\cdot 0$ of such a triangle in the Leech lattice is a maximal subgroup of structure $U_6(2){:}S_3$, the $U_6(2)$ fixing all three vectors and the S_3 naturally permuting them. Elements of the form $\zeta_T\epsilon_\Omega$ fix each v_k whenever $\{i, j\} \subset T$. Clearly any permutation in the pointwise stabiliser of $\{i, j\}$ under the action of M_{24}, which has structure M_{22}, will also fix each v_k. Again, clearly no Golay codeword will fix these three vectors. We define a *duad* to be any set of size two $D \subseteq \Omega \setminus \{i, j\}$ and define a *duad element* to be any element of the form $\theta_D := \zeta_{D\cup\{i,j\}}\epsilon_\Omega$. Again, since ϵ_Ω is central we have:

Corollary 7 *$\theta_A\theta_B = \theta_B\theta_A$ if and only if $A \cup B \subseteq H \in \mathcal{S}(3,6,22)$.*

Whilst the sporadic groups $Co_1 (\cong \cdot 0/Z(\cdot 0))$ and Co_2 are exceptional in their nature, the classical group $U_6(2)$ is part of a well-behaved infinite family. Since connections between unitary groups and design theory are well established (see for instance [11], [10]) it seems likely that similar results to those presented here for other groups may be possible.

Finally we again note that just as theorem 3 was characteristic free, the two corollaries given above will hold independent of the characteristic of the representation.

6 Concluding Remarks

The results of this paper were originally observed for elements of the form $\zeta_T\epsilon_\Omega$ using the relation of Figure 8 which was employed by Bray and Curtis in [1] to construct $\cdot 0$ using the techniques of 'symmetric generation'.

Acknowledgments

The author is grateful for the financial support received from EPSRC for the duration of his PhD during which this work was done. I am deeply indebted to my PhD supervisor Professor Rob Curtis for his continuing guidance and support throughout these investigations without which this paper would not have been possible.

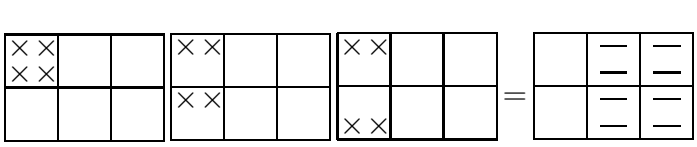


Figure 8: The relation satisfied by the elements $\zeta_T \epsilon_\Omega$

References

[1] J.N. Bray and R.T. Curtis "The Leech Lattice, Λ and the Conway Group $\cdot 0$ Revisited" *to appear in the Transactions of the AMS.*

[2] J.H. Conway "A perfect group of order 8,315,553,613,086,720,000 and the Sporadic Simple Groups" Proc. Nat. Ac. Sci. USA **61** (1968), 398-400.

[3] J.H. Conway "A group of order 8,315,553,613,086,720,000" Bull. London Math. Soc., **1** (1969), 79-88.

[4] J.H. Conway "Three lectures on exceptional groups" from "Finite simple groups" (Ed. MB Powell and G Higman) Academic Press, New York, (1971)

[5] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker and R.A. Wilson "An ATLAS of finite groups", OUP (1985).

[6] J.H. Conway and N.J.A. Sloane "Sphere Packing, Lattices and Groups" third edition Springer-Verlag, New York, (1998).

[7] R.T. Curtis "On the Mathieu Group M_{24} and Related Topics" PhD Dissertation, University of Cambridge, June, 1972.

[8] R.T. Curtis and B.T. Fairbairn "Symmetric Representation of the Elements of the Conway Group $\cdot 0$" J. Symb. Comp., **44** (2009) 1044-1067

[9] J. Leech "Notes on sphere packings" Canad. J. of Math. **19** (1967), pp.251-267.

[10] A. Munenasa "Spherical 5-designs obtained from finite unitary groups" European J. Combin. **25:2**, 261-267 (2004). doi:10.1016/S0195-6698(03)00111-2

[11] M.E. O'Nan "Automorphisms of Unitary Block designs" J. Algebra **20**, 495-511 (1972).